



Paxton-Fear, Katie ORCID logoORCID: <https://orcid.org/0000-0002-4472-8955>, Hodges, Duncan and Buckley, Oliver (2019) Increasing the accessibility of NLP techniques for Defence and Security using a web-based tool. In: Defence and Security Doctoral Symposium, 10 November 2019 - 11 November 2019, online.

Downloaded from: <https://e-space.mmu.ac.uk/627527/>

Version: Presentation

Publisher: Cranfield University

Please cite the published version

<https://e-space.mmu.ac.uk>



Increasing the Accessibility of NLP Techniques for Defence and Security using a Web-Based Tool

Katie Paxton-Fear K.Paxton-Fear@cranfield.ac.uk

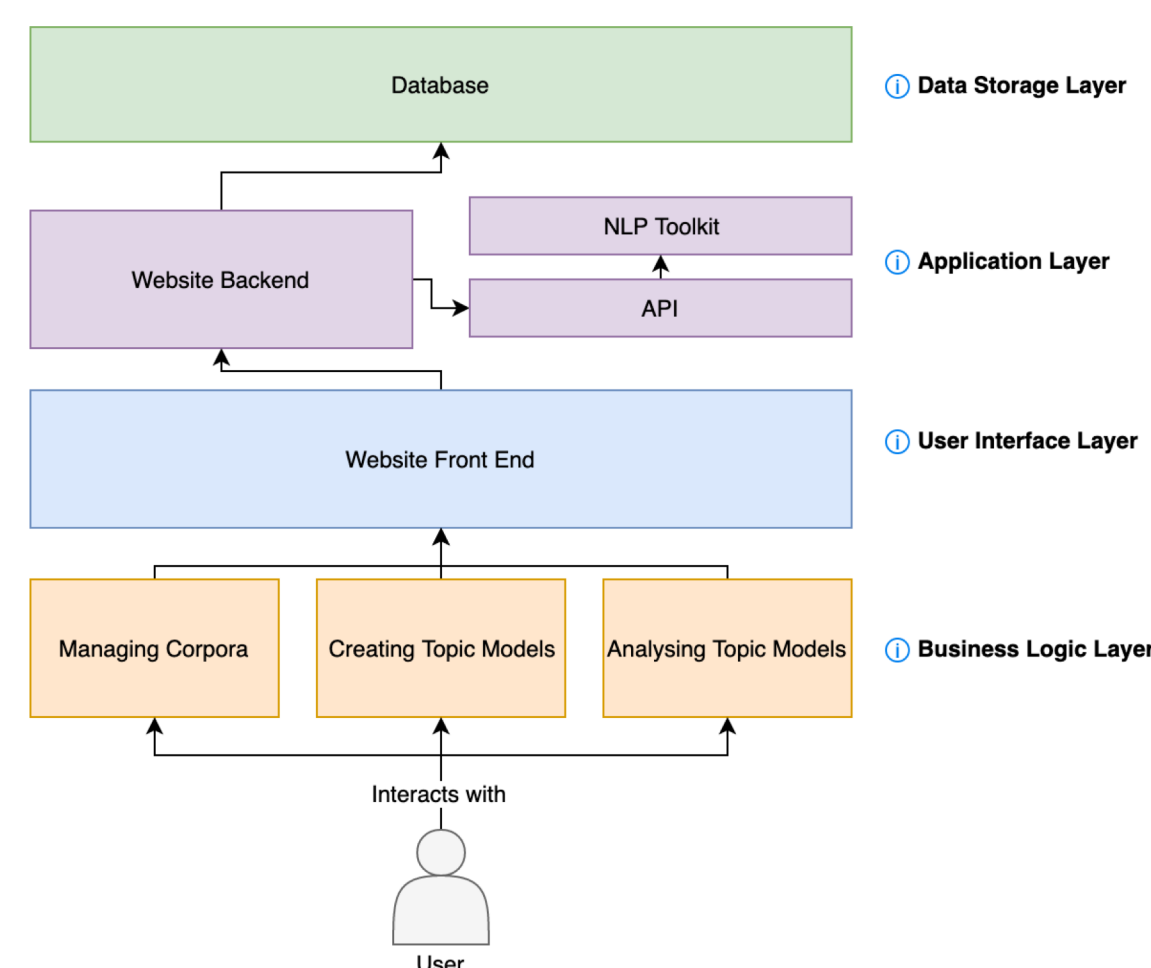
What is Natural Language Processing (NLP)?

NLP techniques are the mechanisms by which a machine can process and analyse text written by humans. These methods are used for a range of tasks including categorising documents, translation and summarising text. To accomplish this a large volume of text (corpus) is collected, processed and finally models can be trained on the corpus. With current methods, the ability to manage corpora is rarely considered, instead relying on researchers and practitioners to do this manually in their file system. To train models, researchers write code directly for one task or experiment, limiting their reusability and ability to generalise.

The Problem: Low Accessibility

Although machine learning (ML) and natural language processing is becoming more common in Defence and Security, there are issues limiting its use. One such issue is the multidisciplinary nature of Defence and Security, with individuals from many backgrounds contributing to a single project. ML and NLP techniques require distinct specialisms to create and interpret a model. This is even more important when delivering research, where outputs may be operationalised and the accessibility can be a limiting factor in their deployment and use, limiting the impact of the work.

Solving the Problem



Managing Corpora

#	Name	Documents Pattern	Metadata Pattern	Folder	Sentence Split Corpus
2	perspectives	*?txt		/Users/katie/OneDrive/Documents/perspectives/	/Users/katie/OneDrive/Documents/perspectives-split/
1	definitelyT	*?txt	*?json	/Users/katie/OneDrive/Documents/def-insider-threat/	/Users/katie/OneDrive/Documents/sentence-split/
3	probablyT	*?txt	*?json	/Users/katie/OneDrive/Documents/all-articles/	

The corpora library allows a user to complete basic operations, including: creating a new corpus, changing the settings of an existing corpus and exploring the documents within a corpus. In addition it allows for complex topic modelling specific operations such as splitting a corpus into sentences and traversing a corpus.

Details

Name: definitelyT

Folder: /Users/katie/OneDrive/Documents/def-insider-threat/

Documents Pattern: *?txt

Metadata Pattern: *?json

Buttons: [Upload] [Delete]

Metadata

Documents: 2098

Models Trained: 0

Create a New Corpus

Name: [input]

Folder: /Users/Default/Default/My-Data

Documents Pattern: *?txt

Metadata Pattern: *?json

Buttons: [Close] [Add]

Traverse the Corpus

The corpus has been traversed, but you can't traverse it if you have added more documents, this will also delete all the sentences and they must be retrained again.

[Re-Traverse Corpus]

Split Corpus into Sentences

Once we trained all the documents in the corpus we can split these into individual sentences.

[Split into Sentences]

Delete Corpus

A corpus that describes where the documents are structured, see [here](#) for more info.

[Delete this corpus]

5c814851af09	5c88f8eb2d622
5c88f8eb2d622	A woman who works for a company was stealing from them for over 18 years, she was well-loved and appreciated by her colleagues to the point where her bosses allowed her and her team to be excused from using the new system. Her workmates always thought she was a bit weird but still loved her, and it came as a surprise that she was stealing from the company. She was caught out by a bank teller who noticed a discrepancy in one of her cheques, after she was caught out, everybody at the company was required to use the new system - zero exceptions - and she was fined \$1.8 million, even though it was estimated that she stole as much as \$60 million.
5c8798716894	Sentence 1: A woman who works for a company was stealing from them for over 18 years, she was well-loved and appreciated by her colleagues to the point where her bosses allowed her and her team to be excused from using the new system.
5c8798716894	Sentence 2: Her workmates always thought she was a bit weird but still loved her, and it came as a surprise that she was stealing from the company.
5c8798716894	Sentence 3: She was caught out by a bank teller who noticed a discrepancy in one of her cheques, after she was caught out, everybody at the company was required to use the new system - zero exceptions - and she was fined \$1.8 million, even though it was estimated that she stole as much as \$60 million.
5c8798716894	

Jargon

- **Corpus/Corpora** – A body of documents used to create a model
- **API** – A piece of software that is designed to communicate with software rather than being used by a human
- **Training** – The process used to create machine learning models
- **Insider Threats** – Security threats that arise from an organisations own employees rather than externally
- **Topic Models** – An NLP model that attempts to automatically find topics in a piece of text using probabilities and key words

Summary

- Using natural language processing (NLP) tools can be difficult for non-specialists.
- Defence and Security involves many different people with different backgrounds
- Machine learning is becoming more common within the defence and security domain
- Therefore it is necessary to create a tool which offers the same functionality as ad-hoc code but is clear and approachable without requiring specialist skills
- **Solution: Web based tool with R application programming interface (API)**

Creating Topic Models

#	Name	Number of Topics	Directory	Stopwords	Stopword Directory	Trained Corpus
1	event-extraction-50-topic-model	50	/Users/katie/OneDrive/	en/news/custom	/Users/katie/OneDrive/	definitelyT
2	event-extraction-100-topic-model	100	/Users/katie/OneDrive/	en/news/custom	/Users/katie/OneDrive/	definitelyT

Topic Models are models that attempt to split a piece of text into topics, this allows researchers to explore the content of text computationally. The topic model library allows for basic operations such as creating new topic models. However, users can also: import topic models that have already been created, traverse a topic model and delete a topic model. In addition models can be explored by topic and the sentences associated with each topic can be viewed.

Model: event-extraction-50-topic-model

Details

Name: event-extraction-50-topic-model

K value (topic): 50

Directory: /Users/katie/OneDrive/Code/phdEvent5

Stopwords: en/news/custom

Stopword Directory: /Users/katie/OneDrive/Code/phdEvent5

Corpus: definitelyT

Buttons: [Delete this Model]

Traverse the Model

The model has been traversed

Create a New Model

Name: [input]

K value (topic): [input]

Directory: [input]

Stopwords: [input]

Stopword Directory: [input]

Corpus: [input]

Buttons: [Close] [Add]

Topic 50 (file alleg epic patient tics kaiser)	Topic 49 (cooki privaci browser collect supra employee)
Topic 48 (breach file sourc record station access)	Document: 5c6e8b7604128
Topic 47 (employee ohio comput enforc licens count)	The manager was involved in setting up the new IT system so that she could determine whether or not she could still continue her current fraudulent activities without being caught and when she realised this wasn't going to be the case she used her status and known personality to get around the new system and have her whole team exempt to avoid detection / questioning as to why only her and her accomplices required the exemption.
Topic 46 (orleski cambridg user nonquest colleg analytics)	Document: 5c6e9bcbf644c
Topic 45 (protect fax appeal attorney product employee)	The higher management gave her department exemption to not use to system and enforced usage on the rest of the organisation.
Topic 44 (comput alleg employee employ access confident)	
Topic 43 (shell royal dutch hall pic oil)	
Topic 42 (amazon employee defend ident degree comput)	

Analysing Topic Models

Finally topic models can be applied to a corpus and analysed. *The Application Tool* allows a user to apply a model and view the results either:

- At a topic level, viewing sentences assigned a certain topic from different documents
- At a document level viewing how different sentences have been assigned different topics.

The Analysis Tool compares topic models by evaluating the symmetrical difference and the intersection, visualising how different models evaluate the same data.

Apply Model to corpus

Corpus: perspectives

Model: event-extraction-150-topic-model

Buttons: [Close] [Apply]

Sentences	Intersection	Appears With
<div>Corpus: Select a corpus</div> <div>Document: 5c8f8eb2d622</div> <div>Buttons: [View Sentences]</div>	<div>These sentences appear in all the topics selected</div> <ul style="list-style-type: none">• A tax office employee who worked as a middle-manager for more than 18 years committed fraud to the tune of more than \$60 million by writing fraudulent checks.	<div>She had done so over 18 years.</div> <div>The news reports describe her being fined about \$63M, although there is no mention of a custodial sentence.</div> <div>The fraud include a further 9 accomplices, whose roles are still being investigated.</div> <div>It would appear that she may have had other members of staff write the cheques and she could authorise them however this is not confirmed.</div> <div>The manager was involved in setting up the new IT system so that she could determine whether or not she could still continue her current fraudulent activities without being caught and when she realised this wasn't going to be the case she used her status and known personality to get around the new system and have her whole team exempt to avoid detection / questioning as to why only her and her accomplices required the exemption.</div>

Insider Threat

This tool-support has been created as part of a project considering the use of NLP to better understand reports of insider threat attacks. These are security incidents where the attacker is a member of staff or another trusted individual. Insider threat attacks are particularly difficult to defend against due to the level of access these individuals gain during the regular course of their employment. The wider use of these techniques would generate greater impact both tactically in defending against these attacks and strategically in developing policy and procedures. There are tools available, however they are often complex and perform a single-task, limiting their use. To generate maximum impact from our research we have developed this web-based software to make the tools more accessible, especially to non-specialist researchers, customers and potential users.

Katie Paxton-Fear K.Paxton-Fear@cranfield.ac.uk [†], Dr Duncan Hodges d.hodges@cranfield.ac.uk [†],

Dr Oliver Buckley o.buckley@uea.ac.uk [‡]

[†] Cranfield University [‡] University of East Anglia

Centre for Electronic Warfare and Cyber, Cranfield Defence and Security, Defence Academy of the United Kingdom

www.cranfield.ac.uk

[dst1]